

3

35.C15064

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Osamu IWASAKI

Application No.: 09/770,200

Filed: January 29, 2001

For: IMAGE PROCESSING APPARATUS



Examiner: Not Assigned

Group Art Unit: 2852

June 28, 2001

Commissioner for Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

JAPAN

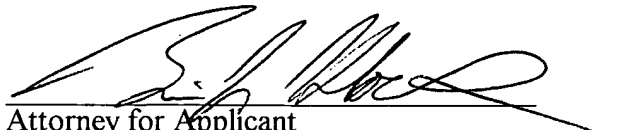
2000-022393

January 31, 2000

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010 All correspondence should continue to be directed to our address given below.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "B. L. Klock", written over a horizontal line.

Attorney for Applicant
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/dc

CF0 15064 US/sug



本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

09/770,248
Osamu Iwasaki
January 29, 200

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 1月31日

出 願 番 号

Application Number:

特願2000-022393

出 願 人

Applicant (s):

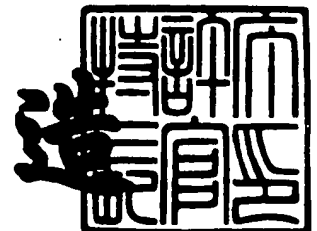
キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 2月23日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 4053002

【提出日】 平成12年 1月31日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 画像データ処理装置、画像データ記録装置、画像データ
記録システム、画像データ記録方法及び記憶媒体

【請求項の数】 12

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会
社内

 【氏名】 岩崎 督

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100090273

 【弁理士】

 【氏名又は名称】 國分 孝悦

 【電話番号】 03-3590-8901

【手数料の表示】

 【予納台帳番号】 035493

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像データ処理装置、画像データ記録装置、画像データ記録システム、画像データ記録方法及び記憶媒体

【特許請求の範囲】

【請求項 1】 偽造防止処理が施された入力画像データに応じた印字 I D を生成して画像データ記録装置に転送する第 1 の転送手段と、

上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像データを暗号化するとともに印字制御コマンド化して印字制御データを生成する印字制御データ生成手段と、

上記印字制御データと上記印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを具備することを特徴とする画像データ処理装置。

【請求項 2】 入力された画像データに偽造防止を含む画像処理を施す画像処理手段と、

上記画像処理手段によって偽造防止処理が施された画像データに応じた印字 I D を生成する印字 I D 生成手段と、

上記印字 I D 生成手段によって生成された印字 I D を画像データ記録装置に転送する第 1 の転送手段と、

上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像処理手段によって所定の処理が施された画像データを暗号化する暗号化手段と、

上記暗号化手段によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する印字制御データ生成手段と、

上記印字制御データ生成手段によって生成された印字制御データと上記印字 I D 生成手段によって生成された印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを具備することを特徴とする画像データ処理装置。

【請求項 3】 上記暗号化手段は、上記共通鍵で生成された変換テーブルを使用して暗号化処理を行うことを特徴とする請求項 2 に記載の画像データ処理装置。

【請求項 4】 画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成手段と、

上記共通鍵生成手段によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理する管理手段と、

上記共通鍵生成手段によって生成された共通鍵を上記画像データ処理装置に送出する共通鍵発行手段と、

上記画像データ処理装置から印字 I D 及び印字制御データが送られてきたときに、上記印字 I D に対応する共通鍵を上記管理手段から取得する共通鍵取得手段と、

上記共通鍵取得手段によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析手段と、

上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段によって取得した共通鍵を用いて復号化する復号化手段と、

上記復号化手段によって復号化された印字画像データを記録媒体に記録する印字手段とを具備することを特徴とする画像データ記録装置。

【請求項 5】 上記共通鍵生成手段は、上記共通鍵を無作為に生成することにより、生成する共通鍵を印字 I D に対応させないことを特徴とする請求項 4 に記載の画像データ記録装置。

【請求項 6】 上記復号化手段は、上記共通鍵で生成された変換テーブルを使用して復号化処理を行うことを特徴とする請求項 4 に記載の画像データ記録装置。

【請求項 7】 偽造防止処理が施された入力画像データに応じた印字 I D を生成して画像データ記録装置に転送する第 1 の転送手段と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像データを暗号化するとともに印字制御コマンド化する印字制御データ生成手段と、上記印字制御コマンド化された印字制御データと上記印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを有する画像データ処理装置と、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成手段と、上記共通鍵生成手段によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理する管理手段と、上記共通鍵生成手段によって生成された共通鍵を上記画像データ処理装置に送出する共

通鍵発行手段と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得手段と、上記共通鍵取得手段によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析手段と、上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段によって取得した共通鍵を用いて復号化する復号化手段と、上記復号化手段によって復号化された印字画像データを記録媒体に記録する印字手段とを有する画像データ記録装置とからなることを特徴とする画像データ記録システム。

【請求項 8】 入力された画像データに偽造防止を含む画像処理を施す画像処理手段と、上記画像処理手段によって偽造防止処理が施された画像データに応じた印字 I D を生成する印字 I D 生成手段と、上記印字 I D 生成手段によって生成された印字 I D を画像データ記録装置に転送する第 1 の転送手段と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像処理手段によって所定の処理が施された画像データを暗号化する暗号化手段と、上記暗号化手段によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する印字制御データ生成手段と、上記印字制御データ生成手段によって生成された印字制御データと上記印字 I D 生成手段によって生成された印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを有する画像データ処理装置と、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成手段と、上記共通鍵生成手段によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理する管理手段と、上記共通鍵生成手段によって生成された共通鍵を画像データ処理装置に送出する共通鍵発行手段と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得手段と、上記共通鍵取得手段によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析手段と、上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段によって取得した共通鍵を用いて復号化する復号化手段と、上記復号化手段によって復号化された印字画

像データを記録媒体に記録する印字手段とを有する画像データ記録装置とからなることを特徴とする画像データ記録システム。

【請求項 9】 偽造防止処理が施された入力画像データに応じた印字 I D を生成して画像データ記録装置に転送する第 1 の転送処理と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像データを暗号化するとともに印字制御コマンド化する印字制御データ生成処理と、上記印字制御コマンド化された印字制御データと上記印字 I D とを上記画像データ記録装置に転送する第 2 の転送処理とを画像データ処理装置が行い、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成処理と、上記共通鍵生成処理によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理手段により管理する管理処理と、上記共通鍵生成処理によって生成された共通鍵を上記画像データ処理装置に送出する共通鍵発行処理と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得処理と、上記共通鍵取得処理によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析処理と、上記解析処理によって抽出された印字画像データを、上記共通鍵取得処理によって取得した共通鍵を用いて復号化する復号化処理と、上記復号化処理によって復号化された印字画像データを記録媒体に記録する印字処理とを画像データ記録装置が行うことを特徴とする画像データ記録方法。

【請求項 1 0】 入力された画像データに偽造防止を含む画像処理を施す画像処理処理と、上記画像処理処理によって偽造防止処理が施された画像データに応じた印字 I D を生成する印字 I D 生成処理と、上記印字 I D 生成処理によって生成された印字 I D を画像データ記録装置に転送する第 1 の転送処理と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像処理処理によって所定の処理が施された画像データを暗号化する暗号化処理と、上記暗号化処理によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する処理と、上記印字制御データ生成処理によって生成された印字制御データと上記印字 I D 生成処理によって生成された印字 I D とを上記画像データ記

録装置に転送する第 2 の転送処理とを画像データ処理装置が行い、

上記画像データ処理装置から転送されてきた印字 ID に基づいて共通鍵を生成する共通鍵生成処理と、上記共通鍵生成処理によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 ID を管理手段により管理する管理処理と、上記共通鍵生成処理によって生成された共通鍵を画像データ処理装置に送出する共通鍵発行処理と、上記画像データ処理装置から送られてくる印字 ID 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得処理と、上記共通鍵取得処理によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析処理と、上記解析処理によって抽出された印字画像データを、上記共通鍵取得処理によって取得した共通鍵を用いて復号化する復号化処理と、上記復号化処理によって復号化された印字画像データを記録媒体に記録する印字処理とを画像データ記録装置が行うことを特徴とする画像データ記録方法。

【請求項 1 1】 上記請求項 1 ～ 8 の何れか 1 項に記載の各手段を構成するプログラムをコンピュータから読み出し可能に記録したことを特徴とする記憶媒体。

【請求項 1 2】 上記請求項 9 または 1 0 に記載の方法を実行するプログラムをコンピュータから読み出し可能に記録したことを特徴とする記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は画像データ処理装置、画像データ記録装置、画像データ記録システム、画像データ記録方法及び記憶媒体に関し、特に、ホストコンピュータで画像処理を行い記録装置で印字を行う記録システムにおける弊紙等の偽造防止に用いて好適なシステムに関する。

【 0 0 0 2 】

【従来の技術】

紙幣及び有価証券等の偽造防止システムの多くは、複写機等のように入出力装置が一体となったシステムである。しかし、今日のパーソナルコンピュータの発

展に追従して、その周辺機器であるスキャナ、デジタルカメラ、プリンタ等の高性能化が目覚しく、複写機以上の高画質の画像を出力することが可能となった。これに伴い、上記の偽造行為も多数発生しており、その防止システムを構築することが求められている。

【0003】

パーソナルコンピュータ環境での偽造防止システムの特徴は、入力装置、出力装置の制御をホストコンピュータが行うため、紙幣及び有価証券等の特定パターンの認識処理をホストコンピュータの画像処理手段に盛り込む必要がある。パーソナルコンピュータにおいては、出力装置の制御コードさえ分かれば特定の画像処理手段を使用しなくても出力作業が可能である。

【0004】

そこで、偽造防止手段を盛り込んだ特定の画像処理手段以外の使用を避ける手段として、出力装置の制御コードを暗号化する方法が有用である。上記のような方法はパーソナルコンピュータ環境ではないが、例えば、特開平6-105141号で開示されている。この方法を、パーソナルコンピュータ環境に適応させると、図2に示すようになる。

【0005】

図2において、ステップS2001～ステップS2005は、ホストコンピュータにおける処理であり、ステップS2006からステップS2009は記録装置本体における処理である。

【0006】

まず、最初のステップS2001で「OS（基本ソフトウェア）」、もしくはアプリケーションより画像データを入力する。次に、ステップS2002で偽造防止を含む画像処理を行う。上記ステップS2002の画像処理は、カラーマッチングやガンマの補正等と量子化で構成され、印字画像データに変換される。このステップS2002での偽造防止は、一般的にはパターン識別による特定画像の判断を行い、上記特定画像の場合に画像データに欠陥を施す処理となる。

【0007】

次に、画像処理された印字データをステップS2003において暗号化する。

この暗号化された印字データをステップ S 2004 でプリンタ本体を制御する印字制御データにコマンド化する。

【0008】

上記のコマンド化された印字制御データを、ステップ S 2005 でデータの転送回路（不図示）を制御（実際に制御を行うのは「OS」でもよい。）して、プリンタ本体に転送する。

【0009】

次に、プリンタ本体のステップ S 2006 の処理において、印字制御データを受信する。この受信した印字制御データを、ステップ S 2007 でコマンド解析の処理を行い、暗号化されている印字画像データを生成する。

【0010】

次に、この暗号化されている印字画像データをステップ S 2008 の復号化処理によって印字データに変換する。そして、この復号化された印字データをステップ S 2009 において記録媒体に印字する。

【0011】

【発明が解決しようとする課題】

しかしながら、上記のシステムはホストコンピュータとプリンタ本体との間において暗号化しているが、入力画像に対するプリンタに転送するデータが 1 対 1 に対応するため、暗号の解読が容易となっている。

【0012】

すなわち、従来のシステムで行われているプリンタの制御コードが未公開であるのと同様であり、画像の偽造防止を有効に行うことができない問題があった。

本発明は上述の問題点にかんがみ、入力画像に対する偽造防止を有効に行うことができるシステムを構築することを目的とする。

【0013】

【課題を解決するための手段】

本発明の画像データ処理装置は、偽造防止処理が施された入力画像データに応じた印字 ID を生成して画像データ記録装置に転送する第 1 の転送手段と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像データを暗号化

するとともに印字制御コマンド化して印字制御データを生成する印字制御データ生成手段と、上記印字制御データと上記印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを具備することを特徴としている。

また、本発明の他の特徴とするところは、入力された画像データに偽造防止を含む画像処理を施す画像処理手段と、上記画像処理手段によって偽造防止処理が施された画像データに応じた印字 I D を生成する印字 I D 生成手段と、上記印字 I D 生成手段によって生成された印字 I D を画像データ記録装置に転送する第 1 の転送手段と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像処理手段によって所定の処理が施された画像データを暗号化する暗号化手段と、上記暗号化手段によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する印字制御データ生成手段と、上記印字制御データ生成手段によって生成された印字制御データと上記印字 I D 生成手段によって生成された印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを具備することを特徴としている。

また、本発明のその他の特徴とするところは、上記暗号化手段は、上記共通鍵で生成された変換テーブルを使用して暗号化処理を行うことを特徴としている。

【 0 0 1 4 】

本発明の画像データ記録装置は、画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成手段と、上記共通鍵生成手段によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理する管理手段と、上記共通鍵生成手段によって生成された共通鍵を上記画像データ処理装置に送出する共通鍵発行手段と、上記画像データ処理装置から印字 I D 及び印字制御データが送られてきたときに、上記印字 I D に対応する共通鍵を上記管理手段から取得する共通鍵取得手段と、上記共通鍵取得手段によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析手段と、上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段によって取得した共通鍵を用いて復号化する復号化手段と、上記復号化手段によって復号化された印字画像データを記録媒体に

記録する印字手段とを具備することを特徴としている。

また、本発明の他の特徴とするところは、上記共通鍵生成手段は、上記共通鍵を無作為に生成することにより、生成する共通鍵を印字 I D に対応させないことを特徴としている。

また、本発明のその他の特徴とするところは、上記復号化手段は、上記共通鍵で生成された変換テーブルを使用して復号化処理を行うことを特徴としている。

【 0 0 1 5 】

本発明の画像データ記録システムは、偽造防止処理が施された入力画像データに応じた印字 I D を生成して画像データ記録装置に転送する第 1 の転送手段と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像データを暗号化するとともに印字制御コマンド化する印字制御データ生成手段と、上記印字制御コマンド化された印字制御データと上記印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを有する画像データ処理装置と、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成手段と、上記共通鍵生成手段によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理する管理手段と、上記共通鍵生成手段によって生成された共通鍵を上記画像データ処理装置に送出する共通鍵発行手段と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得手段と、上記共通鍵取得手段によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析手段と、上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段によって取得した共通鍵を用いて復号化する復号化手段と、上記復号化手段によって復号化された印字画像データを記録媒体に記録する印字手段とを有する画像データ記録装置とからなることを特徴としている。

また、本発明の他の特徴とするところは、入力された画像データに偽造防止を含む画像処理を施す画像処理手段と、上記画像処理手段によって偽造防止処理が施された画像データに応じた印字 I D を生成する印字 I D 生成手段と、上記印

字 I D 生成手段によって生成された印字 I D を画像データ記録装置に転送する第 1 の転送手段と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像処理手段によって所定の処理が施された画像データを暗号化する暗号化手段と、上記暗号化手段によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する印字制御データ生成手段と、上記印字制御データ生成手段によって生成された印字制御データと上記印字 I D 生成手段によって生成された印字 I D とを上記画像データ記録装置に転送する第 2 の転送手段とを有する画像データ処理装置と、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成手段と、上記共通鍵生成手段によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理する管理手段と、上記共通鍵生成手段によって生成された共通鍵を画像データ処理装置に送出する共通鍵発行手段と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得手段と、上記共通鍵取得手段によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析手段と、上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段によって取得した共通鍵を用いて復号化する復号化手段と、上記復号化手段によって復号化された印字画像データを記録媒体に記録する印字手段とを有する画像データ記録装置とからなることを特徴としている。

【 0 0 1 6 】

本発明の画像データ記録方法は、偽造防止処理が施された入力画像データに応じた印字 I D を生成して画像データ記録装置に転送する第 1 の転送処理と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像データを暗号化するとともに印字制御コマンド化する印字制御データ生成処理と、上記印字制御コマンド化された印字制御データと上記印字 I D とを上記画像データ記録装置に転送する第 2 の転送処理とを画像データ処理装置が行い、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成処理と、上記共通鍵生成処理によって生成された共通鍵及び上記

画像データ処理装置から転送されてきた印字 I D を管理手段により管理する管理処理と、上記共通鍵生成処理によって生成された共通鍵を上記画像データ処理装置に送出する共通鍵発行処理と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得処理と、上記共通鍵取得処理によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析処理と、上記解析処理によって抽出された印字画像データを、上記共通鍵取得処理によって取得した共通鍵を用いて復号化する復号化処理と、上記復号化処理によって復号化された印字画像データを記録媒体に記録する印字処理とを画像データ記録装置が行うことを特徴としている。

また、本発明の他の特徴とするところは、入力された画像データに偽造防止を含む画像処理を施す画像処理処理と、上記画像処理処理によって偽造防止処理が施された画像データに応じた印字 I D を生成する印字 I D 生成処理と、上記印字 I D 生成処理によって生成された印字 I D を画像データ記録装置に転送する第 1 の転送処理と、上記画像データ記録装置から送られてきた共通鍵を用いて、上記画像処理処理によって所定の処理が施された画像データを暗号化する暗号化処理と、上記暗号化処理によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する処理と、上記印字制御データ生成処理によって生成された印字制御データと上記印字 I D 生成処理によって生成された印字 I D とを上記画像データ記録装置に転送する第 2 の転送処理とを画像データ処理装置が行い、

上記画像データ処理装置から転送されてきた印字 I D に基づいて共通鍵を生成する共通鍵生成処理と、上記共通鍵生成処理によって生成された共通鍵及び上記画像データ処理装置から転送されてきた印字 I D を管理手段により管理する管理処理と、上記共通鍵生成処理によって生成された共通鍵を画像データ処理装置に送出する共通鍵発行処理と、上記画像データ処理装置から送られてくる印字 I D 及び印字制御データに対応する共通鍵を上記管理手段から取得する共通鍵取得処理と、上記共通鍵取得処理によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する解析処理と、上

記解析処理によって抽出された印字画像データを、上記共通鍵取得処理によって取得した共通鍵を用いて復号化する復号化処理と、上記復号化処理によって復号化された印字画像データを記録媒体に記録する印字処理とを画像データ記録装置が行うことを特徴としている。

【 0 0 1 7 】

本発明の記憶媒体は、上記に記載の各手段を構成するプログラムをコンピュータから読み出し可能に記録したことを特徴としている。

また、本発明の他の特徴とするところは、上記に記載の方法を実行するプログラムをコンピュータから読み出し可能に記録したことを特徴としている。

【 0 0 1 8 】

【作用】

本発明は上記技術手段を有するので、画像データ処理装置により、画像データ記録装置に印字を行わせる際に、上記画像データ記録装置を制御する印字制御データが、上記画像データ記録装置により発行された共通鍵によって暗号化されているので、記録画像を生成するためには、上記共通鍵を生成した画像データ記録装置を使用しなければならないことにより、不特定多数の画像データ記録装置によって印字処理が行われることを有効に防止できることができる。

【 0 0 1 9 】

【発明の実施の形態】

（第 1 の実施形態）

以下、図面を用いて本発明の画像データ処理装置、画像データ記録装置、画像データ記録システム、画像データ記録方法及び記憶媒体の実施形態を詳細に説明する。

【 0 0 2 0 】

図 1 は、本発明の記録システムにおけるデータ処理の手順を説明したフローチャートである

【 0 0 2 1 】

図 1 において、ステップ S 1 0 0 1 ～ステップ S 1 0 0 0 4、及びステップ S 1 0 0 9 ～ステップ S 1 0 1 2 はホストコンピュータにおける処理である。また

、ステップ S 1 0 0 5 からステップ S 1 0 0 8、及びステップ S 1 0 1 3 からステップ S 1 0 1 7 は、記録装置本体側で行われる処理である。

【 0 0 2 2 】

まず、最初のステップ S 1 0 0 1 で画像データを入力する。次に、ステップ S 1 0 0 2 で偽造防止処理を含む画像処理を行う。

次に、ステップ S 1 0 0 3 で印字 I D の生成を行い、その後、ステップ S 1 0 0 4 で印字 I D を記録装置本体に転送する。

【 0 0 2 3 】

次に、ステップ S 1 0 0 5 で、記録装置本体は印字 I D を受信し、上記受信した印字 I D をステップ S 1 0 0 6 で記憶して確保する。

次に、ステップ S 1 0 0 7 で共通鍵の生成を行う。この際に、記録装置本体は上記印字 I D と共通鍵とが対（ペア）になるように管理する。

【 0 0 2 4 】

また、ステップ S 1 0 0 7 において共通鍵を生成する場合は無作為に行い、共通鍵を印字 I D に対応させないようにする。

次に、ステップ S 1 0 0 8 で上記共通鍵をホストコンピュータに伝送する。

【 0 0 2 5 】

上記記録装置本体から伝送された共通鍵は、ステップ S 1 0 0 9 においてホストコンピュータで受信される。これにより、ホストコンピュータの印字 I D の転送に応答して記録装置本体が共通鍵を発行する形になるため、ステップ S 1 0 0 4 における印字 I D の転送は共通鍵発行の請求を兼ねていることになる。

【 0 0 2 6 】

次に、ステップ S 1 0 1 0 において、ステップ S 1 0 0 2 の処理で生成された印字画像データを、上記ステップ S 1 0 0 9 で受信した共通鍵で暗号化する。

次に、ステップ S 1 0 1 1 において、上記暗号化された印字画像データを印字制御コマンド化する。次に、ステップ S 1 0 1 2 において、上記印字 I D とコマンド化された印字制御データとを記録装置本体側に転送する。

【 0 0 2 7 】

次に、ステップ S 1 0 1 3 において、記録装置本体は印字 I D と印字制御デー

タを受信する。その後、ステップ S 1 0 1 4 に進み、上記受信した印字 I D に対応する共通鍵を、管理している印字 I D と共通鍵の対より検索して取得する。次に、ステップ S 1 0 1 5 に進んで印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する。

【 0 0 2 8 】

次に、ステップ S 1 0 1 6 に進み、ステップ S 1 0 1 4 で取得した共通鍵を用いて印字画像データを復号化する。次に、ステップ S 1 0 1 7 において印字画像データを記録媒体に記録する印字処理を行う。

【 0 0 2 9 】

なお、上述したステップ S 1 0 1 2 とステップ S 1 0 1 3 における印字データの転送処理と、ステップ S 1 0 1 5 ～ステップ S 1 0 1 7 の処理は、順次繰り返して並列に行うようにしてもよい。また、図 1 には記していないが、ステップ S 1 0 1 7 の印字処理を終了した後、使用した印字 I D とそれと対をなす共通鍵を破棄するようにしてもよい。

【 0 0 3 0 】

図 3 は、ステップ S 1 0 1 0 で行われる暗号化処理の内容を説明するフローチャートである。

本実施形態における乱数テーブルは、0 ～ 2 5 5 の整数値（1 バイト長）を不規則に並べた数列で構成している。すなわち、テーブルサイズは 2 5 6 バイトとなる。共通鍵は「0」から「2 5 5」の整数とした。

【 0 0 3 1 】

まず、ステップ S 3 0 0 1 において、乱数テーブルをホストコンピュータのメモリ（RAM）上に格納する。次に、ステップ S 3 0 0 2 において、共通鍵を用いてメモリ（RAM）上の乱数テーブルを暗号化テーブルに変換する。

【 0 0 3 2 】

次にステップ S 3 0 0 3 に進み、上記生成された暗号化テーブルを用いて印字画像データを暗号化する。この場合、印字画像データを 1 バイトずつ順次読み込み、この読み込んだ 1 バイトのデータ値を暗号化テーブルの先頭アドレスからのオフセット分として、該当するアドレスの数値を暗号化印字画像データとする。

【 0 0 3 3 】

図 5 は、ステップ S 3 0 0 2 で行われる処理を説明したフローチャートである。

まず、最初のステップ S 5 0 0 0 で処理を開始する。次に、ステップ S 5 0 0 1 で変数 n を「0」に設定する。この変数 n は、後述のステップ S 5 0 0 3 ～ステップ S 5 0 0 5 を 1 0 0 回繰り返すための管理用のカウンタである。

【 0 0 3 4 】

次に、ステップ S 5 0 0 2 で、変数 B に共通鍵の値を代入する。次に、ステップ S 5 0 0 3 に進み、変数 A に変数 B を用いて次の数式 (1) の計算値を代入する。

$$A = (5 \times B + 13) \bmod 256 \quad \cdots (1 \text{ 式})$$

【 0 0 3 5 】

次に、ステップ S 5 0 0 4 で変数 B に変数 A を用いて次の数式 (2) の計算値を代入する。

$$B = (5 \times A + 13) \bmod 256 \quad \cdots (2 \text{ 式})$$

【 0 0 3 6 】

数式 (1) 及び (2) の計算は、線形合同法によって擬似乱数を発作している。すなわち、共通鍵は線形合同法における初期値に利用していることになる。

次に、ステップ S 5 0 0 5 では、上述したステップ S 3 0 0 2 でメモリに格納された乱数の先頭アドレスからのオフセットが A のテーブル値と、オフセットが B のテーブル値を入れ替える処理を行う。次に、ステップ S 5 0 0 6 で n を「1」だけ増加させる。

【 0 0 3 7 】

次に、ステップ S 5 0 0 7 で n が「100」かどうかを判断する。この判断の結果、n が「100」であった場合はステップ S 5 0 0 8 に進み、変換作業を終了する。一方、ステップ S 5 0 0 7 の判断の結果、n が「100」でない場合にはステップ S 5 0 0 3 に進む。

【 0 0 3 8 】

図 4 は、ステップ S 1 0 1 6 で行う暗号化処理の手順を説明するフローチャー

トである。ここで用いられる乱数テーブルは、ステップ S 3 0 0 1 の処理で用いたものと同一のテーブルである。

【 0 0 3 9 】

まず、最初のステップ S 4 0 0 1 において、乱数テーブルを記録装置本体のメモリ（RAM）上に展開する。

次に、ステップ S 4 0 0 2 において、共通鍵を用いてメモリ（RAM）上の乱数テーブルを復号化テーブルに変換する。ここで、変換した復号化テーブルは、上記暗号化テーブルにおける数列の先頭アドレスからのオフセット値と、そのアドレスに格納されている整数値の関係が逆になっている関係にしてある。

【 0 0 4 0 】

例えば、暗号化テーブルの先頭から 2 5 番目の数値が「1 2」であるとする、復号化テーブルの先頭から 1 2 番目の数値は「2 5」になるようにしている（ただし、テーブルの先頭は 0 番目と定義する）。

【 0 0 4 1 】

すなわち、暗号化テーブルは復号化テーブルの逆変換テーブルとなり、暗号化テーブルによる変換を関数 A（）、復号化テーブルによる変換を関数 B（）とすると、

$$a = A(d), d = B(a)$$

の関係になる。

【 0 0 4 2 】

次に、生成された復号化テーブルを用いて、暗号化印字画像データをステップ S 4 0 0 3 で復号化する。ステップ S 4 0 0 3 では、暗号化印字画像データを順次 1 バイトづつ読み込み、この読み込んだ 1 バイトのデータ値を暗号化テーブルの先頭アドレスからのオフセット分として、該当するアドレスの数値を印字画像データとする。

【 0 0 4 3 】

図 6 は、ステップ S 4 0 0 2 の処理を説明したフローチャートである。

図 6 において、ステップ S 6 0 0 0 ～ステップ S 6 0 0 7 は、ステップ S 5 0 0 0 ～ステップ S 6 0 0 7 と同一の暗号化テーブルの変換作業である。暗号化テ

ーブル作成後、ステップ S 6 0 0 8 においてアドレス値とテーブル値とを入れ替えて復号化テーブルに変換する。

【 0 0 4 4 】

下記の表 1、表 2、表 3 は、本実施形態で使用もしくは生成したテーブルである。

【 0 0 4 5 】

【表 1】

乱数テーブル

x	R(x)	x	R(x)	x	R(x)	x	R(x)	x	R(x)	x	R(x)	x	R(x)	x	R(x)	x	R(x)
0	88	32	184	64	24	96	120	128	216	160	56	192	152	224	248		
1	197	33	165	65	133	97	101	129	69	161	37	193	5	225	229		
2	230	34	70	66	166	98	6	130	102	162	198	194	38	226	134		
3	139	35	107	67	75	99	43	131	11	163	235	195	203	227	171		
4	196	36	36	68	132	100	228	132	68	164	164	196	4	228	100		
5	225	37	193	69	161	101	129	133	97	165	65	197	33	229	1		
6	114	38	210	70	50	102	146	134	242	166	82	198	178	230	18		
7	71	39	39	71	7	103	231	135	199	167	167	199	135	231	103		
8	112	40	208	72	48	104	144	136	240	168	80	200	176	232	16		
9	61	41	29	73	253	105	221	137	189	169	157	201	125	233	93		
10	62	42	158	74	254	106	94	138	190	170	30	202	126	234	222		
11	67	43	35	75	3	107	227	139	195	171	163	203	131	235	99		
12	92	44	188	76	28	108	124	140	220	172	60	204	156	236	252		
13	217	45	185	77	153	109	121	141	89	173	57	205	25	237	249		
14	74	46	170	78	10	110	106	142	202	174	42	206	138	238	234		
15	127	47	95	79	63	111	31	143	255	175	223	207	191	239	159		
16	136	48	232	80	72	112	168	144	8	176	104	208	200	240	40		
17	181	49	149	81	117	113	85	145	53	177	21	209	245	241	213		
18	150	50	246	82	86	114	182	146	22	178	118	210	214	242	54		
19	251	51	219	83	187	115	155	147	123	179	91	211	59	243	27		
20	244	52	84	84	180	116	20	148	116	180	212	212	52	244	148		
21	209	53	177	85	145	117	113	149	81	181	49	213	17	245	241		
22	34	54	130	86	226	118	66	150	162	182	2	214	98	246	194		
23	183	55	151	87	119	119	87	151	55	183	23	215	247	247	215		
24	160	56	0	88	96	120	192	152	32	184	128	216	224	248	64		
25	45	57	13	89	237	121	205	153	173	185	141	217	109	249	77		
26	238	58	78	90	174	122	14	154	110	186	206	218	46	250	142		
27	179	59	147	91	115	123	83	155	51	187	19	219	243	251	211		
28	140	60	236	92	76	124	172	156	12	188	108	220	204	252	44		
29	201	61	169	93	137	125	105	157	73	189	41	221	9	253	233		
30	250	62	90	94	186	126	26	158	122	190	218	222	58	254	154		
31	239	63	207	95	175	127	143	159	111	191	79	223	47	255	15		

【 0 0 4 6 】

【表 2】

暗号化テーブル

x	A(x)	x	A(x)	x	A(x)	x	A(x)	x	A(x)	x	A(x)	x	A(x)	x	A(x)
0	217	32	57	64	24	96	249	128	89	160	56	192	25	224	121
1	197	33	196	65	164	97	132	129	100	161	68	193	36	225	229
2	183	34	70	66	119	98	215	130	55	162	151	194	38	226	87
3	154	35	122	67	75	99	43	131	26	163	250	195	218	227	186
4	165	36	5	68	101	100	228	132	37	164	133	196	4	228	69
5	32	37	0	69	224	101	192	133	160	165	128	197	33	229	64
6	35	38	131	70	227	102	67	134	242	166	3	198	99	230	18
7	246	39	214	71	7	103	231	135	118	167	86	199	54	231	22
8	177	40	208	72	113	104	209	136	240	168	145	200	241	232	81
9	156	41	124	73	92	105	60	137	28	169	252	201	220	233	93
10	207	42	47	74	254	106	239	138	79	170	175	202	15	234	222
11	146	43	114	75	82	107	50	139	195	171	163	203	210	235	178
12	253	44	188	76	189	108	29	140	125	172	221	204	61	236	157
13	88	45	185	77	153	109	248	141	216	173	184	205	152	237	120
14	187	46	27	78	123	110	219	142	202	174	155	206	251	238	91
15	127	47	78	79	46	111	14	143	238	175	206	207	174	239	142
16	136	48	233	80	73	112	168	144	9	176	105	208	201	240	41
17	84	49	52	81	20	113	244	145	212	177	180	209	245	241	213
18	150	50	71	82	167	114	182	146	103	178	199	210	39	242	135
19	138	51	106	83	74	115	42	147	10	179	234	211	59	243	170
20	85	52	181	84	21	116	117	148	116	180	53	212	149	244	148
21	144	53	112	85	80	117	48	149	16	181	49	213	17	245	176
22	83	54	130	86	19	118	115	150	162	182	51	214	147	246	243
23	230	55	198	87	166	119	134	151	102	183	23	215	247	247	6
24	97	56	193	88	96	120	129	152	225	184	65	216	161	248	1
25	12	57	236	89	204	121	172	153	140	185	108	217	109	249	77
26	255	58	95	90	191	122	31	154	110	186	223	218	63	250	159
27	179	59	98	91	66	123	34	155	2	187	226	219	194	251	211
28	173	60	13	92	76	124	205	156	45	188	141	220	237	252	44
29	200	61	169	93	137	125	104	157	72	189	40	221	8	253	232
30	235	62	90	94	171	126	11	158	107	190	203	222	58	254	139
31	94	63	62	95	30	127	143	159	111	191	190	223	158	255	126

【0047】

【表 3】

復号化テーブル

x	B(x)	x	B(x)	x	B(x)	x	B(x)	x	B(x)	x	B(x)	x	B(x)	x	B(x)
0	37	32	5	64	229	96	88	128	165	160	133	192	101	224	69
1	248	33	197	65	184	97	24	129	120	161	216	193	56	225	152
2	155	34	123	66	91	98	59	130	54	162	150	194	219	226	187
3	166	35	6	67	102	99	198	131	38	163	171	195	139	227	70
4	196	36	193	68	161	100	129	132	97	164	65	196	33	228	100
5	36	37	132	69	228	101	68	133	164	165	4	197	1	229	225
6	247	38	194	70	34	102	151	134	119	166	87	198	55	230	23
7	71	39	210	71	50	103	146	135	242	167	82	199	178	231	103
8	221	40	189	72	157	104	125	136	16	168	112	200	29	232	253
9	144	41	240	73	80	105	176	137	93	169	61	201	208	233	48
10	147	42	115	74	83	106	51	138	19	170	243	202	142	234	179
11	126	43	99	75	67	107	158	139	254	171	94	203	190	235	30
12	25	44	252	76	92	108	185	140	153	172	121	204	89	236	57
13	60	45	156	77	249	109	217	141	188	173	28	205	124	237	220
14	111	46	79	78	47	110	154	142	239	174	207	206	175	238	143
15	202	47	42	79	138	111	159	143	127	175	170	207	10	239	106
16	149	48	117	80	85	112	53	144	21	176	245	208	40	240	136
17	213	49	181	81	232	113	72	145	168	177	8	209	104	241	200
18	230	50	107	82	75	114	43	146	11	178	235	210	203	242	134
19	86	51	182	83	22	115	118	147	214	179	27	211	251	243	246
20	81	52	49	84	17	116	148	148	244	180	177	212	145	244	113
21	84	53	180	85	20	117	116	149	212	181	52	213	241	245	209
22	231	54	199	86	167	118	135	150	18	182	114	214	39	246	7
23	183	55	130	87	226	119	66	151	162	183	2	215	98	247	215
24	64	56	160	88	13	120	237	152	205	184	173	216	141	248	109
25	192	57	32	89	128	121	224	153	77	185	45	217	0	249	96
26	131	58	222	90	62	122	35	154	3	186	227	218	195	250	163
27	46	59	211	91	238	123	78	155	174	187	14	219	110	251	206
28	137	60	105	92	73	124	41	156	9	188	44	220	201	252	169
29	108	61	204	93	233	125	140	157	236	189	76	221	172	253	12
30	95	62	63	94	31	126	255	158	223	190	191	222	234	254	74
31	122	63	218	95	58	127	15	159	250	191	90	223	186	255	26

【0 0 4 8】

上記表 1 は、本実施形態で用いた乱数テーブルの一例である。また、表 2 は本実施形態で共通鍵が「1 5」の場合の暗号化テーブルである。さらに、表 3 は本実施形態で共通鍵が「1 5」の場合の復号化テーブルである。

【0 0 4 9】

なお、上述した実施形態では、暗号化処理及び復号化処理をテーブル用いた変換方式にした例を示した。これは、演算による変換方式に対して処理的な負荷が少なく済み、印字速度の低下の原因にならないように考慮したためである。

【0 0 5 0】

また、本実施形態で記録装置本体が印字 ID と共通鍵を管理しているため、記録装置本体が複数のホストコンピュータと接続されている場合に、共通鍵を発行した順番によらず、印字制御データを転送してきた順番に従って印字の処理を行うことが可能である。

【 0 0 5 1 】

(その他の実施形態)

上記実施形態では、共通鍵によって乱数テーブルを変換して暗号化テーブルを生成したが、共通鍵自体が暗号化テーブルでもよい。また、共通鍵を合同法におけるパラメータとして用い、擬似乱数の発生により暗号化テーブルを作成してもよい。

【 0 0 5 2 】

また、暗号化テーブルの作成は、共通鍵によって変化すればよく、合同法に限らず平均採中法などでもよい。また、上記実施形態における共通鍵の発行は、不特定の数でならないため、記録装置の内部タイマの値を使用してもよい。

【 0 0 5 3 】

次に、図 7 のブロック図を参照しながら、本発明を実施する画像データ記録システムの構成例を説明する。

図 7 において、7 0 は画像データ処理装置、7 1 はインタフェース、7 2 は画像処理手段、7 3 は印字 I D 生成手段、7 4 は印字 I D 記憶手段、7 5 は第 1 の転送手段、7 6 は暗号化手段、7 7 は印字制御データ生成手段、7 8 は第 2 の転送手段である。

【 0 0 5 4 】

また、8 0 は画像データ記録装置、8 1 はインタフェース、8 2 は共通鍵生成手段、8 3 は管理手段、8 4 は共通鍵発行手段、8 5 は共通鍵取得手段、8 6 は解析手段、8 7 は復号化手段、8 8 は印字手段である。

【 0 0 5 5 】

図 7 に示したように、この画像データ記録システムは、画像データ処理装置 7 0 と画像データ記録装置 8 0 とで構成されており、それぞれに設けられているインタフェース 7 1 及びインタフェース 8 1 を介して種々のデータ及びコマンドを送受信することで画像データ処理装置 7 0 に入力された画像データを画像データ記録装置 8 0 で印字して出力するようになっている。

【 0 0 5 6 】

図 7 において、画像処理手段 7 2 は、入力された画像データに偽造防止を含む

画像処理を施す。また、印字ID生成手段73は、上記画像処理手段72によって偽造防止処理が施された画像データに応じた印字IDを生成する。上記生成された印字IDは、印字ID記憶手段74に記憶されるとともに、第1の転送手段75によって画像データ記録装置80に転送される。

【0057】

暗号化手段76は、上記画像データ記録装置80から送られてくる共通鍵を用いて、上記画像処理手段1によって所定の処理が施された画像データを暗号化する。また、印字制御データ生成手段77は、上記暗号化手段76によって暗号化された印字画像データを印字制御コマンド化して印字制御データを生成する。そして、上記生成された印字制御データと上記印字ID生成手段73によって生成され、印字ID記憶手段74に記憶されている印字IDが第2の転送手段78によって上記画像データ記録装置80に転送される。

【0058】

共通鍵生成手段82は、画像データ処理装置70から転送されてきた印字IDに基づいて共通鍵を生成する。そして、生成された共通鍵、及び上記転送されてきた印字IDが管理手段83のメモリに記憶されて管理される。

【0059】

共通鍵発行手段84は、上記共通鍵生成手段82によって生成された共通鍵を上記画像データ処理装置70に送出する。また、共通鍵取得手段85は上記画像データ処理装置70から、印字ID及び印字制御データが送られてきたときに、上記印字IDに対応する共通鍵を上記管理手段83から取得する。

【0060】

解析手段86は、上記共通鍵取得手段85によって取得された共通鍵を用いて上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する。復号化手段12は、上記解析手段によって抽出された印字画像データを、上記共通鍵取得手段85によって取得した共通鍵を用いて復号化する。そして、上記復号化された印字画像データが印字手段88によって記録媒体（図示せず）に記録される。

【0061】

(本発明の他の実施形態)

本発明は複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダー、プリンタ等）から構成されるシステムに適用しても1つの機器からなる装置に適用しても良い。

【0062】

また、上述した実施の形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（CPUあるいはMPU）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【0063】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0064】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態で説明した機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【0065】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプ

ログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれる。

【 0 0 6 6 】

【発明の効果】

以上説明したように、本発明によれば、画像データ記録装置から発行された共通鍵を用いて印字制御データを暗号化するので、画像データ処理装置が画像データ記録装置を制御して記録画像を生成するためには、上記共通鍵を発行した画像データ記録装置を使用しなければならないこととなり、不特定多数の画像データ記録装置により印字されることを有効に防止することができ、上記画像データ処理装置における偽造防止処理を確実に実行することが可能となった。これにより、紙幣及び有価証券等の偽造を確実に防止することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態における記録システムの動作手順を示すフローチャートである。

【図 2】

従来技術を用いた記録システムにおける暗号化処理の手順を示すフローチャートである。

【図 3】

第 1 の実施形態における暗号化処理の手順を示すフローチャートである。

【図 4】

第 1 の実施形態における復号化処理の手順を示すフローチャートである。

【図 5】

第 1 の実施形態における暗号化テーブル作成処理の手順を示すフローチャートである。

【図 6】

第 1 の実施形態における復号化テーブル作成処理の手順を示すフローチャートである。

【図 7】

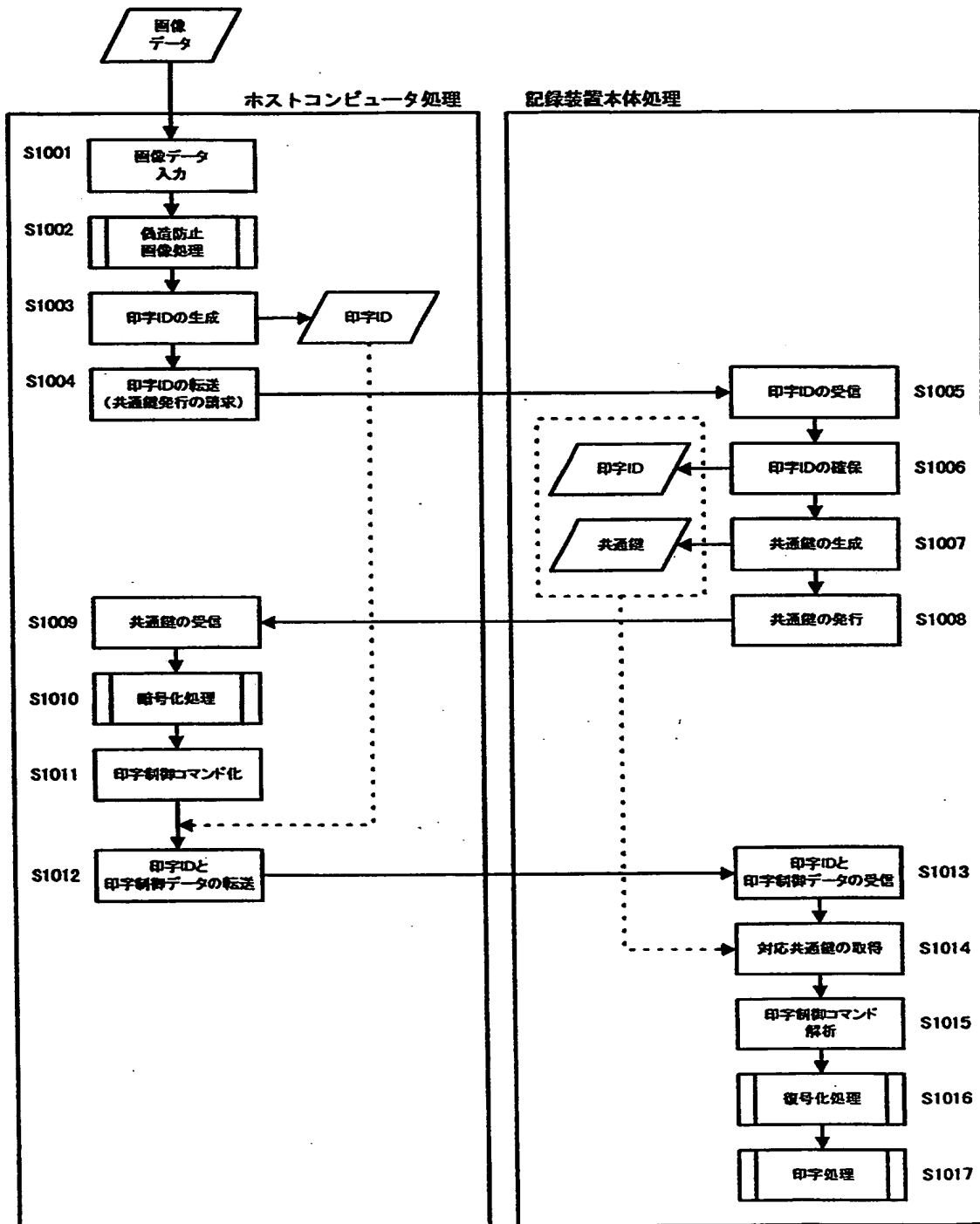
本発明を実現する画像データ記録システムの構成例を示すブロック図である。

【符号の説明】

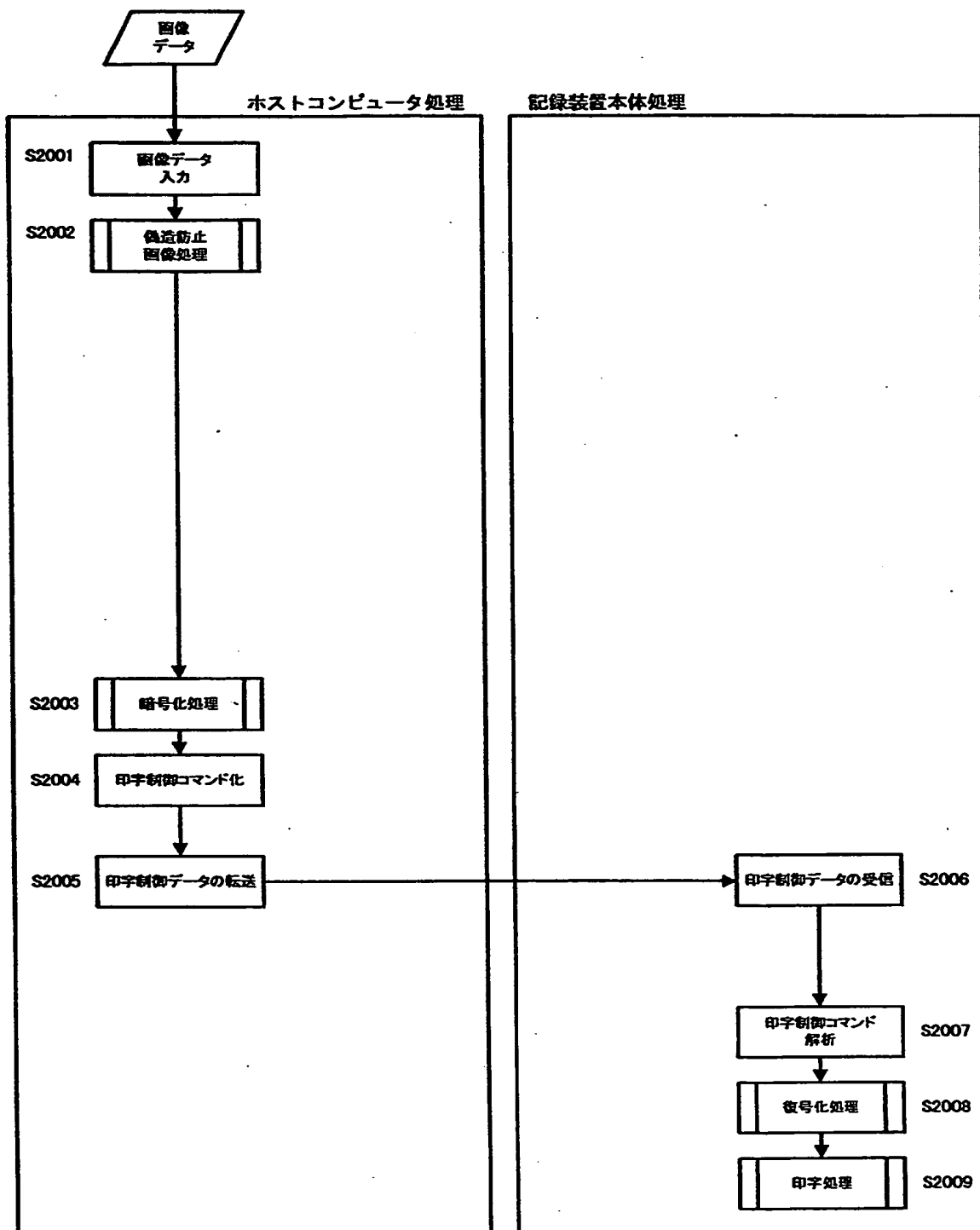
- 7 0 画像データ処理装置
- 7 1 インタフェース
- 7 2 画像処理手段
- 7 3 印字 I D 生成手段
- 7 4 印字 I D 記憶手段
- 7 5 第 1 の転送手段
- 7 6 暗号化手段
- 7 7 印字制御データ生成手段
- 7 8 第 2 の転送手段
- 8 0 画像データ記録装置
- 8 1 インタフェース
- 8 2 共通鍵生成手段
- 8 3 管理手段
- 8 4 共通鍵発行手段
- 8 5 共通鍵取得手段
- 8 6 解析手段
- 8 7 復号化手段
- 8 8 印字手段

【書類名】 図面

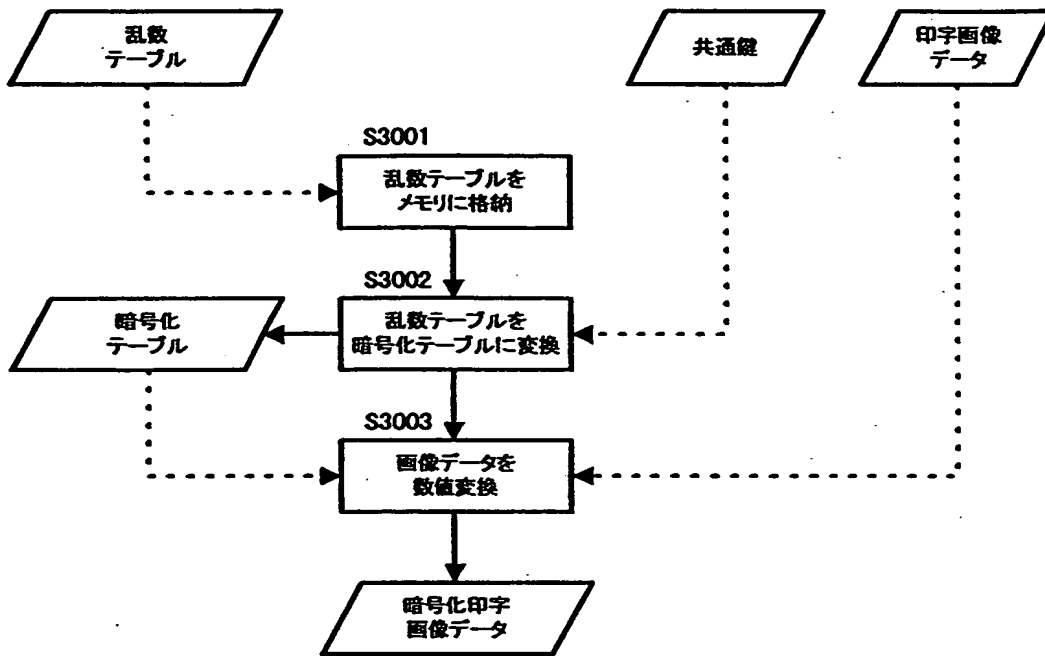
【図 1】



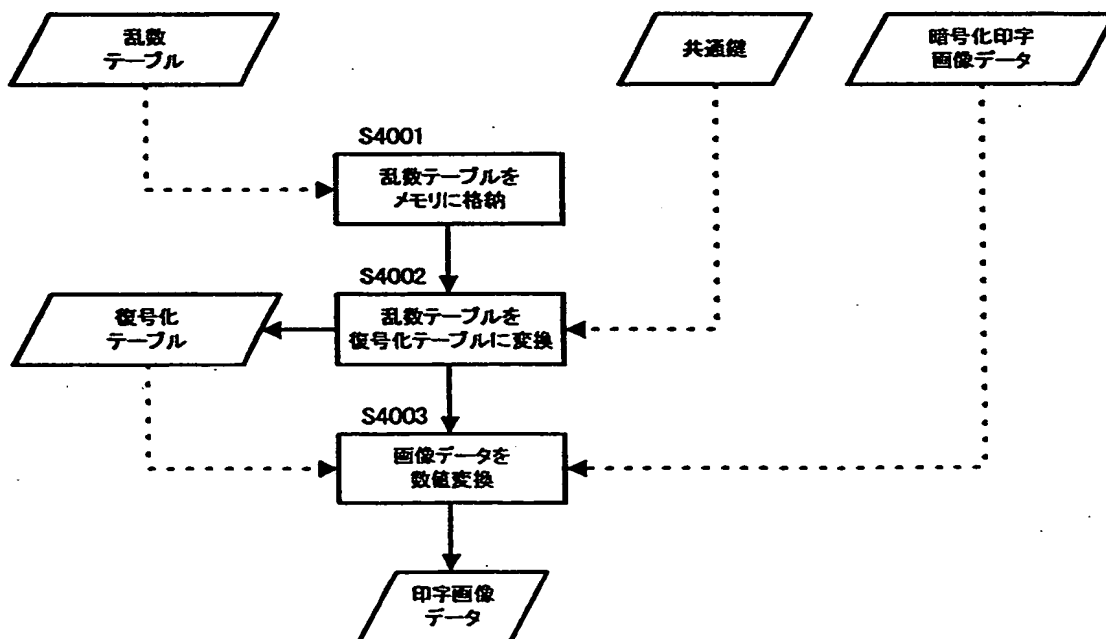
【図 2】



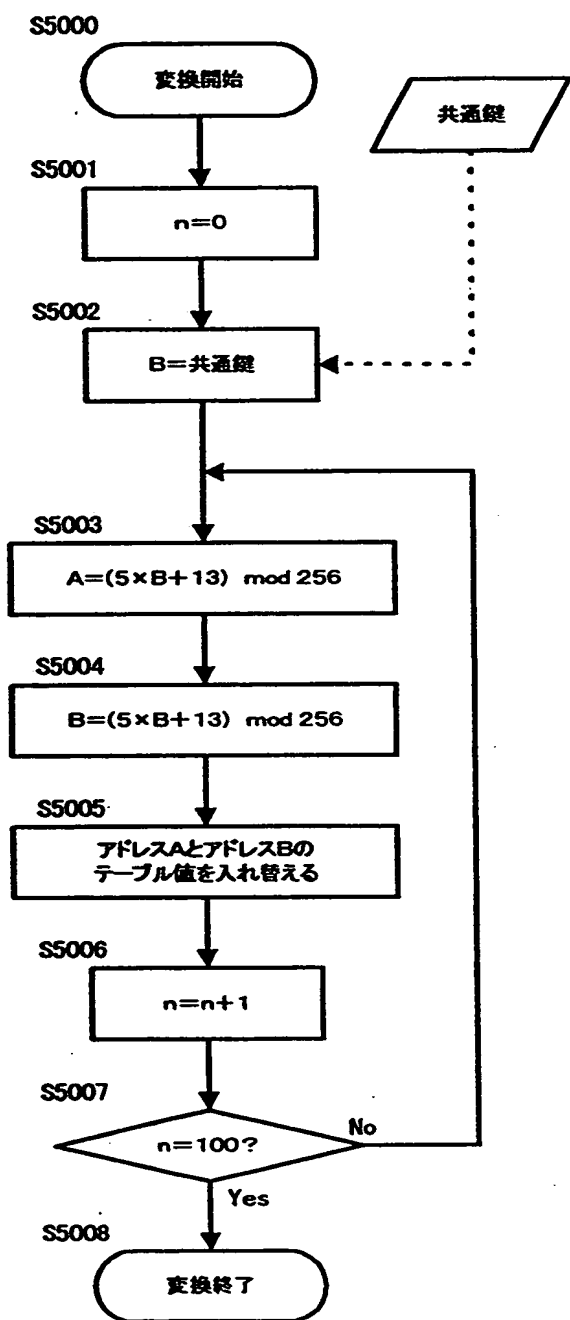
【図 3】



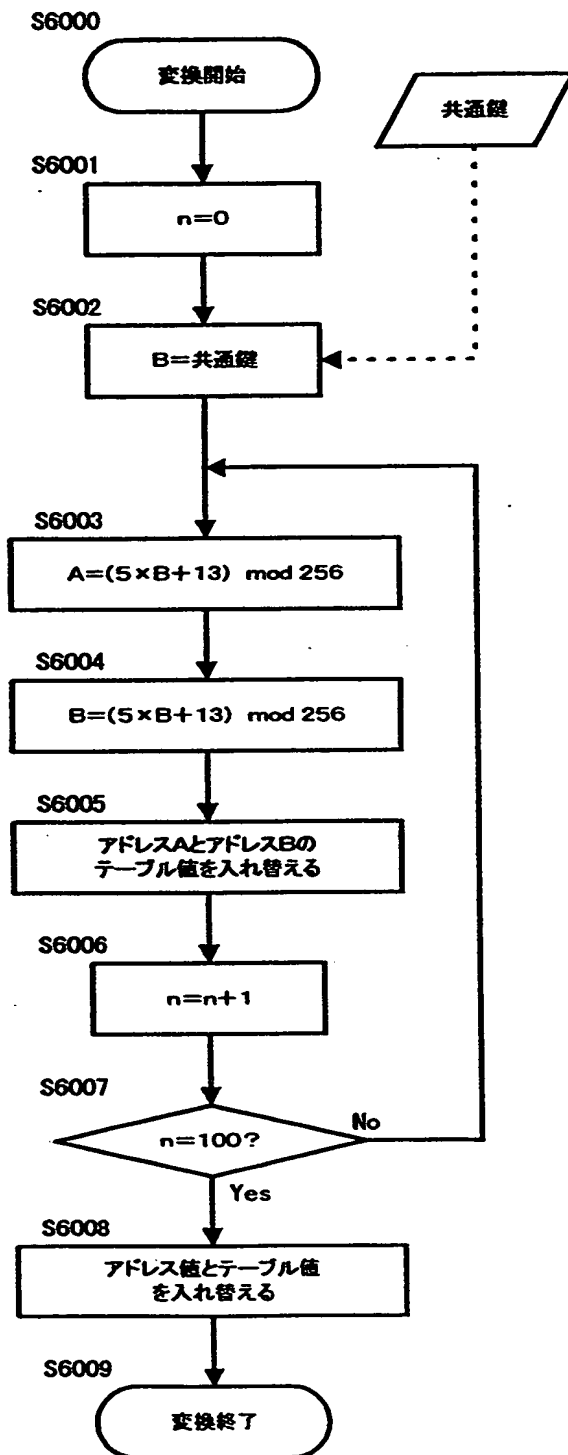
【図 4】



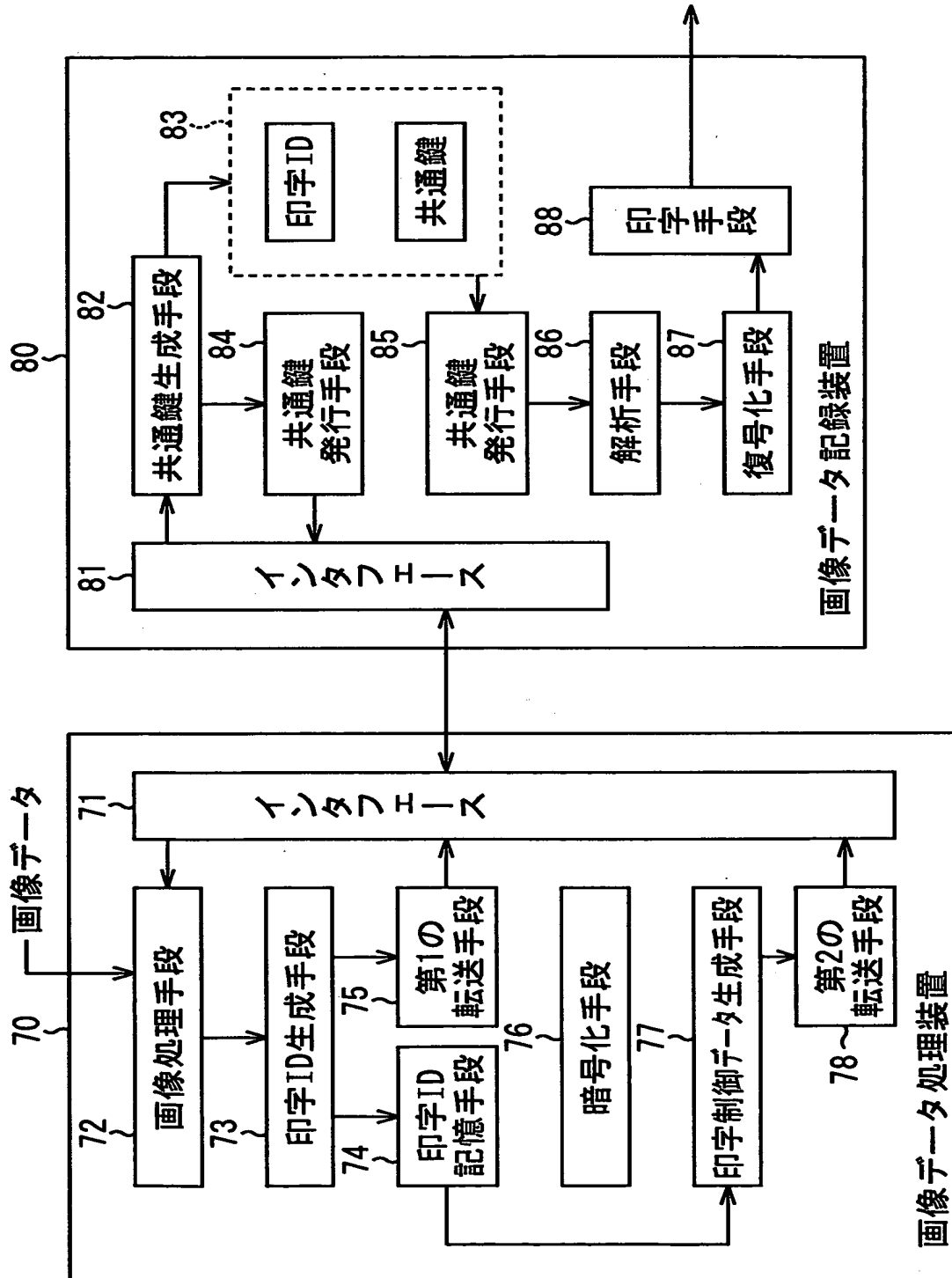
【図5】



【図 6】



【図7】



【書類名】 要約書

【要約】

【課題】 入力画像に対する偽造防止を有効に行うことができるようにする。

【解決手段】 偽造防止処理が施された入力画像データに応じた印字 I D を生成する処理、画像データ記録装置から送られてきた共通鍵を用いて上記画像データを暗号化及び印字制御コマンド化する処理、上記印字制御コマンド化した印字制御データと上記印字 I D とを転送する処理とを画像データ処理装置が行い、上記転送されてきた印字 I D に基づいて共通鍵を生成する処理、上記生成した共通鍵を上記画像データ処理装置に送出する処理、上記印字制御データのコマンドを解析し、暗号化された印字画像データを抽出する処理、上記抽出した印字画像データを、上記共通鍵を用いて復号化する処理、上記復号化した印字画像データを記録媒体に記録する印字処理とを画像データ記録装置によって行うことにより、不特定多数の画像データ記録装置によって印字処理が行われなくようにする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号

氏 名 キヤノン株式会社